View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Ulster University's Research Portal

International Journal of Wireless Networks and Broadband Technologies
Volume 9 • Issue 1 • January-June 2020

Automation of Detection and Fault Management Response of Common Last-Mile Loss-Of-Connectivity Outages Within the Access Network

Alban Scribbins, Open University, Milton Keynes, UK
Kevin Curran, Ulster University, London, UK

ABSTRACT

The article to assesses whether it may be possible to recommend a solution to enable automation of the process of detection and fault management of common conclusive loss-of-connectivity last-mile outages, within the access network. To ascertain the utility of the research, UK based MPLS VPN managed service providers, their fault management staff and their business customers, were surveyed using online questionnaires for their views. UK public Internet users were additionally surveyed via five UK Internet forums. UK communication providers offering MPLS VPN solutions were characterised. Access network connectivity technologies and fault management functions were compared, contrasted and analysed. An aspiration for the solution to be beneficial to the largest potential population, meant that current non-proprietary Internet Standard technologies were selected, justified and identified which could be recommended for use. It was found that of the participating survey respondents, two-thirds were in favour of automation. Many current communication provider processes were found to be mostly automated. The article concludes with recommendations of how an automated solution could potentially be enabled. This involves further use of business-to-business interfacing between communication providers, automation of their Fault Management Systems and introducing Bi-Directional forwarding for detection between last-mile active network elements.

KEYWORDS

Internet, MPLS, Network Management, VPN

1. INTRODUCTION

In the field of Internet connectivity and wide-area-networking, communication providers (CPs) should not be complacent about the need to ensure end-to-end connection availability for connectivity services supplied to their customers. It was reported in October 2013 that a number of businesses lost critical voice and data services, when storms knocked down several telephone poles in the local access network. One company was quoted, “So far it has cost us over £6,000 since losing the connection” (Knowles, 2013). Geographically, access networks (T822a, 2003) reach most rural and

DOI: 10.4018/IJWNBT.2020010101

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Kevin Curran (kj.curran@ulster.ac.uk) Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

urban areas. Often utilising legacy national telephony infrastructure, an access network connects with a regional communication network at a point-of-presence (POP) location, often a local telephone exchange. Within a POP, or within a specialised cabinet deep within the access network, aggregation node equipment is used to converge single customer connections onto shared trunk cabling. The communications infrastructure between the CP aggregation node and the customer premises is known as the 'last-mile'. Many businesses and the general public are unlikely to invest in last-mile backup connections due to the expense involved. Occasionally a customer may experience a last-mile loss-of-connectivity outage and need to contact their CP (Jin et al, 2010). A CP fault management team then initiates manually selected tests in an attempt to diagnose the cause of the outage. Many outages are caused by common conclusive faults (Bendouda and Haffaf, 2019). The process of verbally informing CPs of outages and the manual fault management functions undertaken by CP engineers potentially increase the outage restoration time by days. Outages incur costs. The sooner an outage is detected and resolved the lower the costs incurred (Ayoubi, 2018).

The main justification for the research is based on the benefits to wide area network (WAN) connectivity users. Not all business customers are able to afford to build resilience into their national and international networks. Resilience is expensive (Wosinska and Chen, 2009) and often used for 'high value' sites. For example, national store chains such a charity shops, may not afford to have last-mile backup links to each of their sites. Customers or users of the last-mile connection may experience loss of trade, connectivity to organisational central data processing systems, telephony, staff productivity, staff confidence in WAN network administration and loss of client confidence. The CP may experience compensation payments resulting from breached Service Level Agreement (SLA), blighted brand reputation, loss of investor (Bharadway et al., 2009) and customer confidence. And costs incurred due to incorrectly instigated engineering visits. The cost is relative to the time and duration of the outage (Lyons et al., 2012). These costs may be mitigated by removing the need for customers to contact their CP and for CP fault management staff to manually diagnose common last-mile outages. With an automated solution a last-mile customer could be assured the CP would diagnose last-mile connectivity outages on their connection without being contacted and be assured that last-mile outages may be dealt with promptly and efficiently. In addition, with an automated solution a CP could reduce compensation payments (Hajdarbegovic, 2013) for breached SLAs, arrange for more timely repairs and reduce mistaken engineer call outs and remove basic tedious common diagnostic tasks from fault management staff processes permitting them to spend more time on complex fault issues. Opposition may come from proprietary fault management system manufacturers who may have designed automated systems based on specific underlying high value connectivity technologies such as Ethernet. Access network equipment manufacturers may not accept the value to be gained in adding additional functionality to their devices. CPs may not realise the savings to be gained in introducing more automation to their business environment. Fault management staff may fear for their roles due to the introduction of automation.

Therefore, this research is focused on United Kingdom based, last-mile fixed-line WAN access network connectivity technologies and topologies. These technologies may transmit data and/or voice traffic. The discussion focuses primarily on the powered (active) elements utilised within last-mile connections located between the customer premises equipment and a CPs POP equipment including elements such as aggregation node equipment. Only last-mile connectivity outages are researched. Other connectivity issues such as performance will not be included. Metallic leased lines are not included as they are being phased out by fibre Ethernet (Ofcom, 2012). The research is restricted to investigating only those CPs involved in the provision and fault management assurance of last-mile and access network connections which are physical media connectivity CPs, wholesale connectivity CPs and managed service providers (MSP) who offer Multi-Protocol Label Switching (MPLS) virtual private networks (VPN) solutions to business customers (Nyasulu et al., 2018). Primary data has been sourced from organisations providing and using MPLS/IP VPN solutions that may have at least one MPLS VPN connected site in the UK. Detailed discussion of MPLS and MPLS VPN is out-of-scope.

Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

IP VPN is synonymous with MPLS VPN (Stenbjerg et al., 2018. In addition, primary data has been sourced from UK Public Internet users, who may have experienced Internet connectivity outages and were required to contact their ISP to have diagnostic tests initiated. Focus on human processing is limited to fault management functions with regard to last-mile connectivity outages. Back-office equipment used by CP organisations in the management of last-mile outages is also summarised.

Often for CP fault management staff to become aware of a customer last-mile outage, the customer reports the outage to the CP (Jin et al., 2010). This act alone extends the restoration time. A connection outage experienced outside normal working hours may be undetected and unacknowledged by user and CP potentially for days. Once the CP fault management staff are aware of the outage they are required to process the fault (Kompella et al., 2010). Invariably they will run common standard diagnostic tests in order to identify the issue. Human fallibility (Jin et al., 2010) can result in test delays and incorrectly selected tests. Low cost connections may have outage diagnostics initiated only within CP standard working hours. The 'current system' where customers need to report a last-mile outage and CP fault management need to manually select and run diagnostic tests is very inefficient and potentially costly to all the directly affected stakeholders. An alternative would be to automate the current system to increase efficiency and reduce costs for those stakeholders. A proposed automated system may also be found to be beneficial in other data networking contexts, where communications between two end-points may fail and require fault management assurance to be implemented. This could potentially be of value to all CPs and all Internet and WAN customers alike (Singh et al., 2017; Rios et al., 2017). In an attempt to assist the largest number of potential beneficiaries globally, a low-cost automated solution is required (Beckett et al., 2017). Re-inventing the wheel would be astronomically expensive. Designing new technologies may result in limited distribution due to proprietary constraints. Changing nothing benefits no-one. This research seeks to identify the already largely automated current last-mile fault management functions and processes, establish where automated improvements can be attained and suggest low cost non-proprietary Internet Standard technologies that may be utilised to enable an automated solution.

2. BACKGROUND

High severity errors are dominated by connectivity problems with third-party ISPs (Turner et al., 2012). Sundaresan et al., (2011) and Lee and Kim (2012) base studies on the measurement of network characteristics. Traffic performance factors such as packet loss, jitter, throughput and latency in digital subscriber line (DSL) networks are the focus of Sundaresan et al., (2011) which is unrelated to the loss of connectivity problem field researched in this study. Lee and Kim (2012) examine all types of connectivity issues experienced by users, such as application errors, configuration problems as well as loss-of-connectivity outages. Both studies are related in that they are set within access networks alike this study. (Turner et al., 2012; Sundaresan et al., 2011; Lee and Kim, 2012) use measurements from various sources for evaluation and to base their conclusions upon. This research does not follow the same format, it concentrates on examining access network detection methods and CP fault management processes. Of interest in the latter two studies is the use of embedding code on the user's host pc (Lee and Kim, 2012) and host gateway (Sundaresan et al., 2011) to take measurements. Embedding code is also a method used by Kim et al., (2011) and Sullivan et al., (2009) to run applications with regard to network issues. Kim et al., (2011) propose DYSWIS, an inference and expert knowledge system used to diagnose issues that are not "simple network connectivity problems". It could be argued that DYSWIS could not diagnose "loss of physical connectivity" issues at all due to the end user's 'diagnosis module' being orphaned from the WAN 'DHT network' during a physical connectivity outage. Of greater relevance is a patent submitted by Sullivan et al., (2009) which includes the use of embedded code in the user's host pc and gateway devices. The design appears primarily a system that attempts to establish whether the fault is on the local network rather than between customer and CP. It does not resolve the "hands-off" goal of this study, for if the cause is not located and resolved, a call

Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

is still necessary to the CP by the customer. Both Sullivan et al. (2009) and Jin et al. (2010) describe similar problem situations to this research. NEVERMIND (Jin et al., 2010) is an interesting operational proactive, inference and expert knowledge tool which attempts to resolve "customer edge" problems in advance of them occurring. Alike the Turner et al., (2012) paper, Jin et al. (2010) utilise a large collection of customer call ticket information for evaluation. This research takes a reactive approach to failure detection and management and acknowledges how useful a tool NEVERMIND could be for CP's and their customers. Proactive fault management solutions already exist for critical high value backhaul and core connections such as those over which MPLS VPNs are supplied (Hussain, 2005; Li and Liang, 2011). In the last decade much work has been conducted in order to guarantee the high availability of MPLS based trunk networks (Minei and Lucek, 2011).

2.1. Regulation and Standardisation

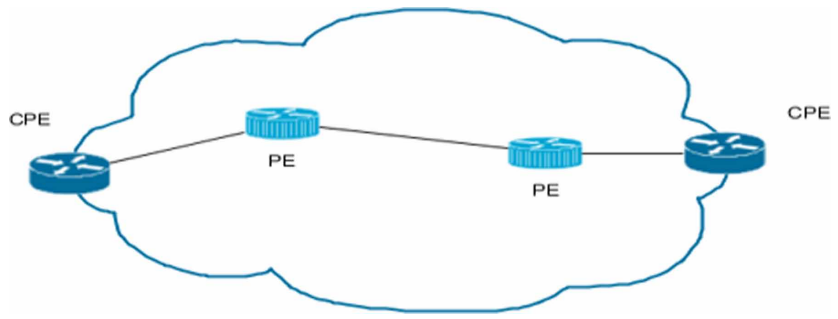
Duties of Ofcom, the UK communication industry regulator, are the product of European Union and UK Parliament legislation. The UK Communications Act 2003 enabled major expansion of competition in the CP sector forcing the separation of the UK national communications infrastructure from the parent company British Telecom into a demarcated subsidiary named Openreach (Ofcom, 2013a). Openreach is now the incumbent access connectivity supplier in the UK and has the responsibility to maintain and provide fair and equal access to the original UK national communications infrastructure for all UK fixed-line CPs (Sabatucci et al., 2017).

Regulation promotes standardisation and vice-versa though the terms do not equate (Holland et al., 2015). Communication industry regulation draw on the capabilities of standardised technologies with which to foster competition to define the scope in which CPs may operate and to encourage technical innovation. UK communication networks are subject to standards agreed by stakeholders associated with the following non-governmental standard setting organisations (SSOs) which include the European Telecommunications Standards Institute (ETSI), International Telecommunications Union (ITU), Internet Engineering Task Force (IETF), International Organisation for Standardisation (ISO) and the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA).

2.2. Multi-Protocol Label Switching Virtual Private Network

MPLS is a transport technology that routes network traffic using labels rather than network addresses (Ghein, 2007; IETF RFC3031, 2001). Utilising labels (Reed, 2003) reduces routing overheads, permits easy separation of multiple customer network traffic over a shared backbone connection and enables an additional level of network security (Lewis and Pickavance, 2006; Gill et al., 2018). An MPLS VPN allows a customer organisation to run a private WAN network over the CPs MPLS backbone (Almofary et al., 2013; IETF RFC4364, 2006). The customer can outsource their whole WAN administration and management to another organisation. In an MPLS VPN topology the underlying last-mile access network connections are abstracted from the customer's view as shown in Figure 1.

Figure 1. Conceptual depiction of an MPLS VPN including connections to VPN sites



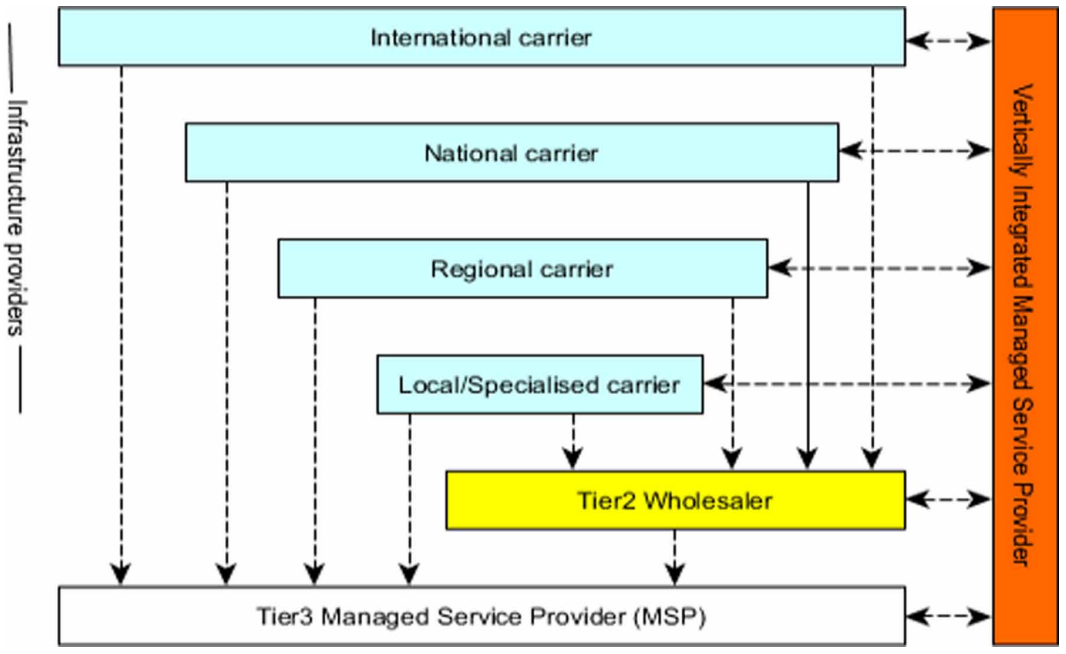
Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

2.3. UK Communications Providers (CPs)

At the physical level infrastructure carriers exist. These organisations provide the actual physical media that fixed-line communications are transported across and have varied geographical scopes – International, National, Regional and Local/specialised. CPs which lease large quantities of physical fixed-line communication connections from national and regional carriers to provide to CPs are referred to as Tier2 Wholesalers. Organisations who offer MPLS VPN managed service solutions to business customers and who supply their VPN customers with access network connectivity products sourced from Tier2 Wholesalers will be referred to as Tier3 Managed Service Providers (MSPs). In order to be as competitive as possible various different tier providers may provide MPLS VPN managed services directly to business customers as well as to lower tier providers. Such organisations are known as vertically integrated managed service providers. Figure 2 is an illustration of the current MPLS VPN MSPs and their relationships to carriers and other tier suppliers.

The provision of communication services operate over a number of virtual layers which broadly follow the conceptual network layering models recommended for interconnection and compatibility between communication systems, the OSI Reference Model and the TCP/IP reference Model (Li et al., 2011; Jones et al., 2003). Carriers and Tier2 Wholesalers who provide physical layer services often including the NTE equipment operate at the lowest network layer. Tier2 Wholesaler may rent physical connections from a carrier, running their own core network above the lowest layer. Tier3 MSP may purchase capacity on a Tier2 Wholesaler's core network for use in their own MPLS backbone network. A network layer above. Tier3 MSP may provide a number of MPLS VPNs to separate business customers all utilising the same MPLS backbone. Additional network layer. The business customer will have a private network addressing scheme for use internally with the MPLS VPN. Top network layer.

Figure 2. UK topology of MPLS VPN MSPs and their infrastructure provider suppliers, the dotted arrows indicate an optional relationship, solid arrows indicate at least a 1:1 relationship



Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

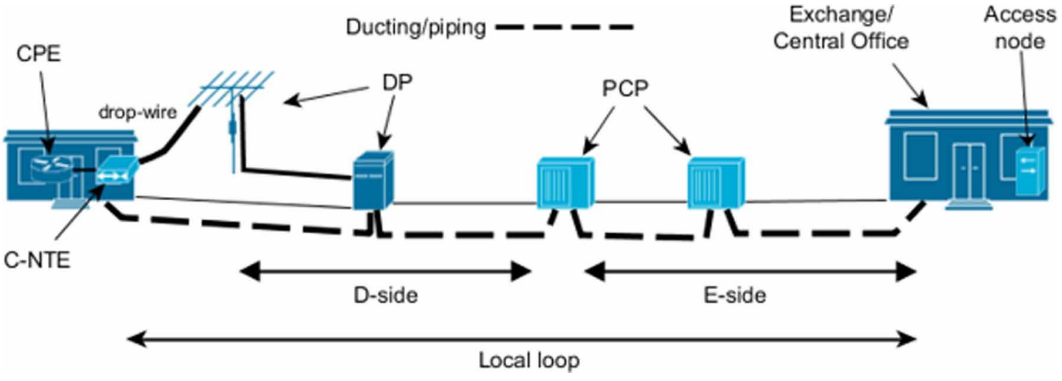
2.4. UK Access Networks, Media and Technologies

The vast majority of UK access connectivity technologies are supplied over the Openreach infrastructure. The next section describes this infrastructure and how it is available for equal use by other UK CPs. The extent to which CPs are able to place their networking equipment within access networks is fairly diverse. For the purposes of this research the focus is primarily on the last-mile infrastructure and the elements within it. Defining a last-mile access connection as the infrastructure between 'customer premises equipment' (CPE), 'customer premises network termination equipment' (C-NTE) and CP 'aggregation node network termination equipment' (A-NTE). Where telephony media is utilised there will additionally be 'passive network termination equipment' (P-NTE) located within the customer premises.

Apart from the Hull area of England, Openreach maintains the legacy telephony fixed-line communications infrastructure in the UK. Openreach refers to the infrastructure between an exchange and customer premises as the 'local loop'. An alternative national access network data and television infrastructure is maintained by the UK national Cable provider, Virgin Media. The Openreach access network primary Point-of-Presence (POP) is often located in a local telephone exchange or 'Central Office' (CO). The local exchange may house access node multiplexing and routing equipment designed for the bi-directional transfer of data with backhaul fibre regional networks. Where data and voice traffic are communicated together the equipment is referred to as a Multi-Service Access Node (MSAN). Openreach demarcates the access network infrastructure into three segments. An E-side (Exchange side) segment refers to infrastructure located between a centrally located exchange and a number of star topology positioned Primary Cross Connection Point (PCPs) cabinets. A D-side (Distribution side) segment refers to the infrastructure between PCP and distribution point (DP). DPs are either street cabinets or telephone poles, generally on the same road as the customer premises. The final segment of infrastructure between a DP and the actual customer premises is referred to as a drop-wire (see Figure 3).

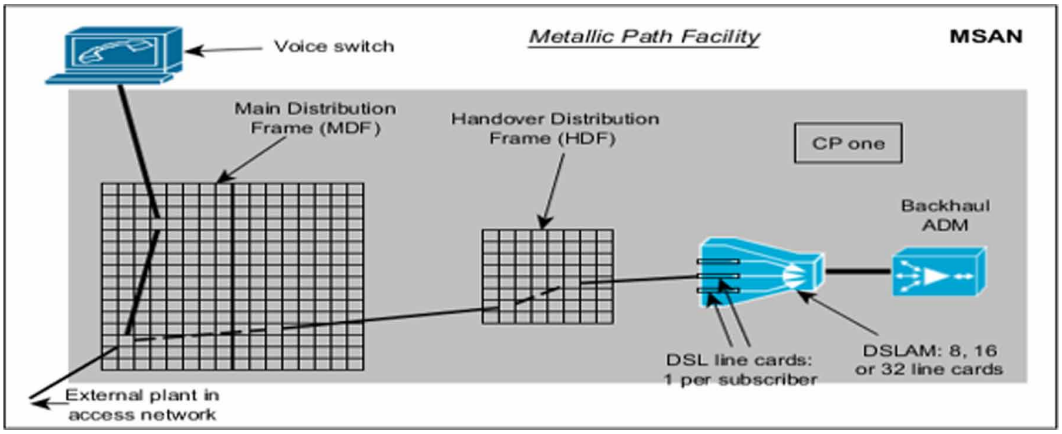
Metallic Path Facility (MPF) refers to the twisted-pair cabling and underlying infrastructure that link a customer premises and the exchange, traditionally used for telephony (Openreach, 2011a). Within the exchange the routing of voice and data traffic is separated by a 'Main Distribution Frame' (MDF) (see Figure 4). Voice traffic is routed to a voice switch and data to a segregated area in the exchange demarcated by a Handover Distribution Frame (HDF). The segregated area contains data transmission equipment owned by other CPs than Openreach. Openreach make available their access network infrastructure for rental by other UK CPs via 'Local Loop Unbundling' (LLU). This allows other CPs to connect their own multiplexing and distribution equipment within the exchange to connect to the Openreach physical media (Openreach, 2011a).

Figure 3. Conceptual depiction of the Openreach access network



Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

Figure 4. Conceptual depiction of Metallic Path Facility (MPF) within the POP

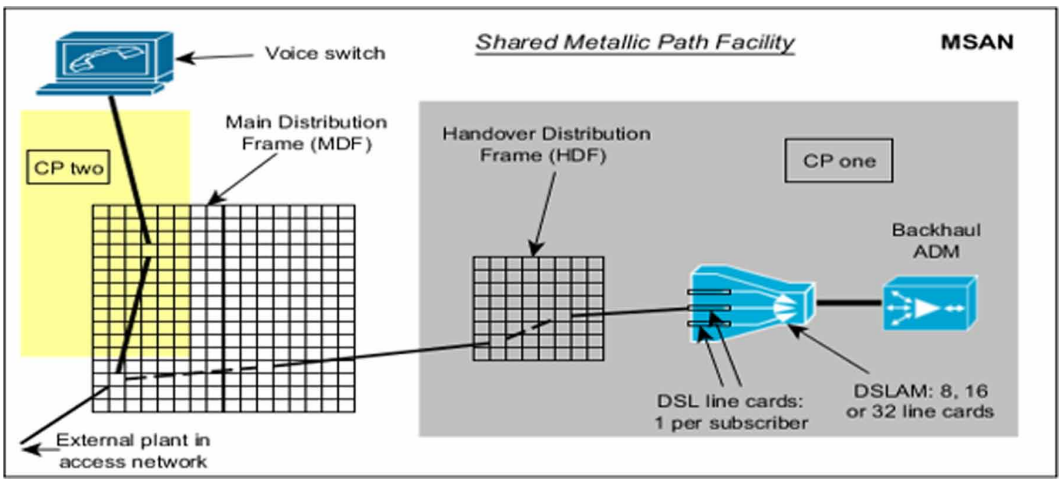


Shared Metallic Path Facility (SMPF) has been bought in by Ofcom to allow different CPs to supply telephony and standard broadband over the same Openreach MPF. Openreach supply the physical infrastructure but two alternative CPs than Openreach each supply either voice or data traffic (see Figure 5).

MPF cannot be used with NGA Superfast broadband access technologies however, because the length of MPF connections are often outside the acceptable limits for such services to operate. With the onset of NGA technologies such as FTTP, FTTC and EFM, Openreach has enabled CPs to place their own aggregation node equipment as far into the current access network as the distribution points, called 'Sub-Loop Unbundling' (SLU) (see Figure 6). Under the Openreach 'Physical Infrastructure Access' (PIA) scheme, ducting, piping and aerial infrastructure between exchange and DP is available for use to other CPs (Openreach, 2014).

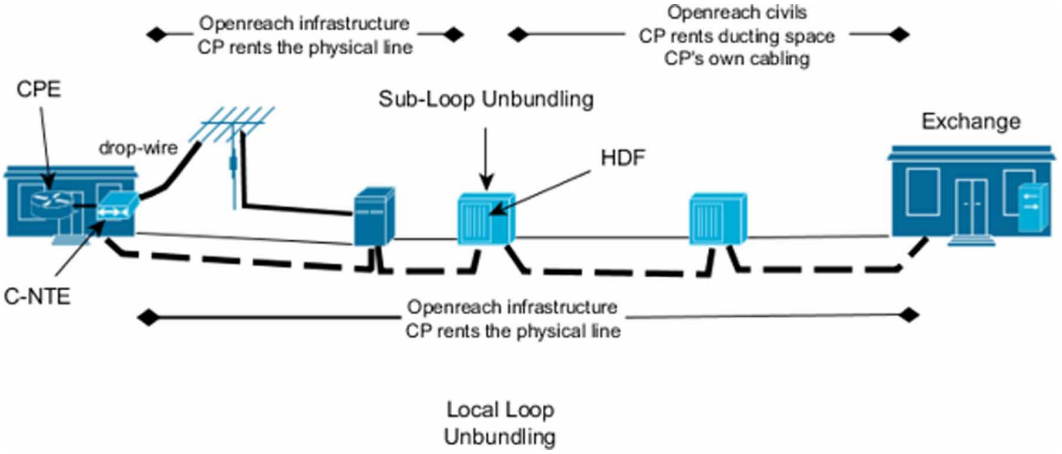
A variation of MPF LLU and SLU utilising Openreach's NGA network infrastructure is 'Virtually Unbundled Local Access' (VULA). The following sections summarise each of the UK access connectivity technologies offered for use with MPLS VPN solutions by UK MSPs. These summaries

Figure 5. Conceptual depiction of Shared Metallic Path Facility (SMPF)



Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

Figure 6. Conceptual depiction of LLU and SLU



relate to Openreach product offerings since many CPs rent Openreach physical access network capacity. Ethernet is the only technology not classed as a broadband service of those products reviewed.

2.5. Access Media and Technologies

2.5.1. Ethernet

Optical fibre Ethernet has replaced legacy copper-based leased lines as the optimum technology for business connectivity. Ethernet is an uncomplicated connectivity technology utilising fibre end-to-end between A-NTE and C-NTE. Recent advances in the standardisation of management and monitoring of Ethernet has meant that it has become viable as a highly available guaranteed service with very stringent service level agreements (SLAs). Due to these stringent SLA guarantees, Ethernet NTE equipment is constantly monitored and managed as standard by the NTE supplier. The A-NTE will normally have specific fault management functionality built in allowing diagnostic testing via a variety of interface options. It is normal for the provider to supply a complete package of hardware equipment and installation (Gunning, 2006; McGuire, 2008; SIN476, 2013).

2.5.2. Ethernet in the First Mile (EFM)

Another Ethernet based service EFM is a combination of fibre and metallic cabling. EFM differs from Ethernet in that most of the infrastructure from CO towards customer premises is fibre-based to the customers most local EFM access-node enabled PCP. From this access-node basic EFM is provided over two pairs of twisted-pair metallic cabling to individual P-NTEs within the customer building after those all lines are terminated at a single SHDSL compatible C-NTE. The multiple metallic pairs provide some resilience if a single pair goes down, resulting in major service degradation rather than total outage. At the access-node A-NTE termination is via a DSL line card or port within a Digital Subscriber Line Access Multiplexer (DSLAM). The DSLAM multiplexes data together from a number of single connections for transport over a single high capacity fibre trunk line. A DSLAM transports traffic bi-directionally. Due to fairly stringent SLAs, EFM circuits are very likely to be monitored and managed constantly by the NTE provider. EFM can be diagnostically tested in the same method as Ethernet from an EFM DSLAM A-NTE towards the C-NTE. Additionally, the metallic pairs can be tested on their own using standard telephony diagnostic tools. EFM DSLAMs are also likely to have built in diagnostic functionality (ITU-T G.991.2, 2005; SIN476, 2013).

Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

2.5.3. Symmetrical Digital Subscriber Line (SDSL)

EFM has taken over as successor of SDSL. SDSL was popular for business in the past as it could attain almost 2Mb symmetrical traffic and was very cheap in comparison to metallic leased lines. The infrastructure of SDSL is almost identical to ADSL. SDSL cannot carry telephony traffic though (ETSI, 2010).

2.5.4. Asymmetrical Digital Subscriber Line (ADSL)

An exchange may contain a number of DSLAMs. DSLAMs from different manufacturers are able to house a number of line cards in slots. Each line card is an A-NTE. At the customer premises the carrier's contractual infrastructure responsibility terminates at the P-NTE. The carrier's last-mile link stretches from CO to P-NTE. An MSP's link may stretch to CPE though. Due to the low cost of ADSL, carriers do not apply proactive monitoring and management to the connection. Each line card can be connected via an MDF to a local or remote diagnostic tool (ITU-T G.992.1, 1999; ITU-T G.992.5, 2009; SIN346, 2011).

2.5.5. Fibre-To-The-Cabinet (FTTC)

Although EFM does not appear to be listed as an NGA technology, it does share many of the infrastructure characteristics of the NGA 'Very High Speed Digital Line Subscriber' (VDSL) technology. VDSL is known as FTTC in the UK. The most marked similarity to EFM is the use of fibre from the CO to a VDSL cabinet in the vicinity of the customer premises, followed by a metallic last-mile cable to the customer premises. The technology incorporates a metallic cable P-NTE and a VDSL2 compatible C-NTE to terminate the customer end of the VDSL line. A DSLAM is also required in the VDSL cabinet alike EFM. The major contrast to EFM is the use of Generic Passive Optical Networking (GPON) for the fibre side of the line, Figure 2.12. This requires an Optical Network Termination unit connected to the VDSL DSLAM within the VDSL cabinet. Analogue voice traffic is routed via metallic twisted-pair to the CO voice switch. Both VDSL and EFM can be provided under the SLU scheme to CPs. It is most likely that proactive monitoring and management is not applied to FTTC circuits by the carrier supplier. The last-mile for EFM and FTTC are from the PCP DSLAM cabinets to the CPE. FTTC utilises telephony testing for the metallic cabling. VDSL shares the NGA optical fibre infrastructure with FTTP and utilises the same end-to-end testing applied to FTTP circuits (ETSI, 2013; SIN476, 2013).

2.5.6. Fibre-To-The-Premises (FTTP)

FTTP is a fully end-to-end optical fibre service utilising Generic Passive Optical Network (GPON) technology. The service has better SLA guarantees than FTTC, ADSL and SDSL because no metallic cable is utilised in the access connection. Fibre is distributed from a GPON enabled exchange, referred to as an NGA node, to an underground location where the optical lines are split up. The Splitter Node (SPN) is the equipment used to split the main fibre into 32 sub-fibres. Each split fibre is then routed via existing Openreach ducting to an underground Tube Manifold access node for green-field sites or to a DP for brown-field sites (Barker, 2009). The fibre is then routed to a Customer Splicing Point (CSP) attached to the customer premises then through a customer's external wall aperture to an internal optical network terminating unit (ONT). FTTP and FTTC have a different access node termination structure than the other broadband and Ethernet technologies. The incoming fibre to the NGA node is passed into an Optical Handover Point (OHP) (Barker, 2009). Further detail is out-of-scope. It is likely that FTTP circuits are monitored by the carrier due to stringent SLA. Diagnostic testing is end-to-end from OHP to the customer end optical network terminating unit (ONT), their C-NTE (ITU-T G984.1, 2008; SIN476, 2013).

Kevin Curran (kj.curran@ulster.ac.uk) Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

2.5.7. Cable

A Cable transmission service provides various converged services over either a fully coaxial cable or hybrid/coaxial (HFC) access network infrastructure. The UK's only cable carrier, Virgin Media, offers MPLS VPN managed services. HFC uses a combination of fibre and metallic physical media. The overall HFC infrastructure is linked together by distribution hubs referred to as 'Headends' (HE). HFC access network infrastructure is a mixture of designs of tree-and-branch or star topology. Within the headend site a number of Cable Modem Termination Systems (CMTS) will connect to customer sites via specialised broadband routers. This is the CP end of the Cable access network. The CMTS has much the same functionality as a DSL DSLAM. In a star topology HFC access network, the infrastructure is connected utilising fibre optic cable. Regional centres (RC), local centres (LC), and district centres (DC) link fibre network rings. District Centres are often street cabinets. Within the DC the data travelling in both directions is transferred to a different physical medium via an Optical Node (ON). From each DC a number of coaxial cables are distributed and the number of connections increased with the use of group amplifiers (GA) and final amplifiers (FA). A final distribution point, either a splitter or tap, separates shared coaxial into individual drop line connections to customer sites. Optical nodes, amplifiers, splitters and taps have no functionality by which to initiate fault notification, they are totally passive. A powered Cable Modem (CM) is required to terminate the coaxial access network at a customer site and has a C-NTE role. Cable diagnostic testing is conducted from the CMTS device at the headend. It is unlikely that the Cable carrier will proactively monitor Cable connections between the optical node and the customer premises (ETSI, 2003).

2.6. Fault Management Within UK Access Networks

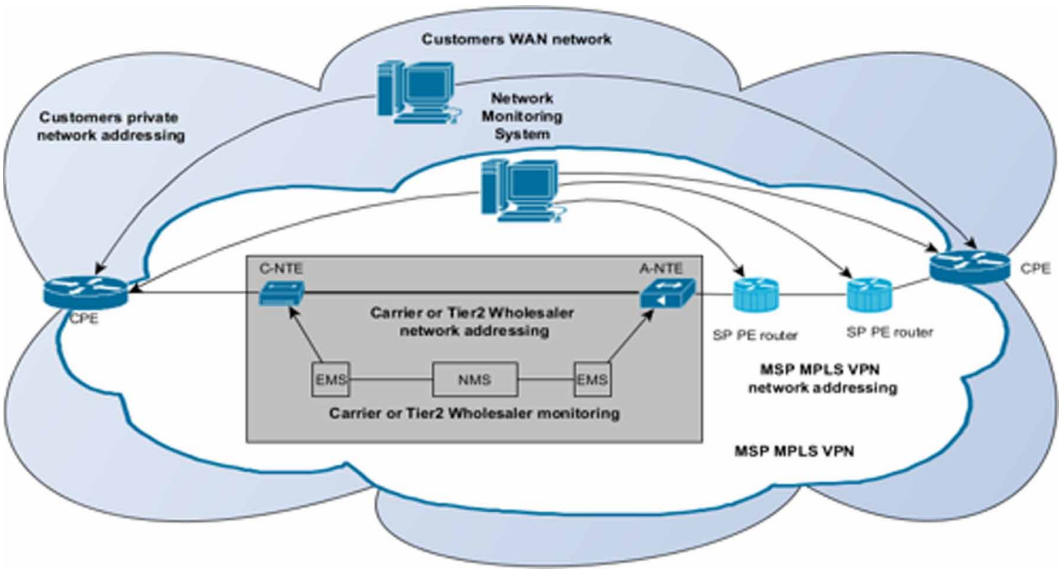
Each access network connection physical media is at risk from human fallibility and extraordinary weather events. Metallic cabling faults are much more common than fibre faults. Overhead cable is at risk from abnormally high vehicles, adverse weather (Knowles, 2013), dislodged poles and tree damage. Underground cable is susceptible to diggers, drilling and water ingress. CP active network element hardware and software may also fail. CP and customer contract a service level agreement (SLA) under which they negotiate terms for each connection which include the expected annual availability (Jones, 2004) and guaranteed repair time. Compensation may be claimed if the time taken to restore the connection exceeds the guaranteed repair time agreed in the SLA (Franke, 2012). Ethernet, EFM and FTTP services are normally monitored by the NTE provider thus outages may be detected quickly and managed promptly. The other technologies do not have the same service guarantees thus monitoring may not be undertaken. Maintaining effective management of diverse customer connections requires complex CP networks and management systems, prompting service assurance guarantees via a set of guidelines under the mnemonic FCAPS. The International Telecommunications Union (ITU) published a set of guidelines that have been used as the basis upon which many CPs and network management system application producers have organised network management and administration functions. The Fault management guidelines include Clause 5.5.2, listing functions to 'act upon error detection notifications, trace and identify faults, carrying out sequences of diagnostic tests and correcting faults' (ITU-T X.700, 1992). Further recommendations have been issued (ITU-T M.3400, 2000). In order to assist the integration of NGA technologies and Ethernet into the access network, a series of standardised functions to assist with fault assurance were introduced under the title 'Operations, Administration and Maintenance (OAM)'. OAM standards (IETF RFC6291, 2011) have enabled the introduction of various functions and tools to be applied at the connection and service level for individual technologies (MEF-17, 2007; ITU-T Y.1731, 2013). These include fault management functionality, specifically concerning monitoring and diagnostics. Monitoring protocols, applications and diagnostic tools have been standardised for use across a variety of the latest access network technologies. OAM fault management functionality is often inbuilt into current NGA and Ethernet NTE devices. This functionality enables monitoring of NTE devices by monitoring protocols and applications.

Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

Monitoring can be undertaken from various diverse locations. Only active (powered) devices can be monitored. Active monitoring makes use of network monitoring system applications to actively contact network elements to confirm connectivity using protocols such as the ping (ICMP) utility. Alternatively, passive monitoring can be utilised using a network management protocol such as Simple Network Management Protocol (SNMP) to either poll the status of a network element or to receive an alert or notification of a change of status from a software agent within the network element (T823, 2004). The inclusion of standardised monitor functionality such as SNMP is ubiquitous in access network active devices. A connection can only be monitored from the same network 'layer' as the monitoring management system resides on. In other words, a carrier can only monitor active elements on the same network level as themselves, but not of their clients or their client's customer's networks. It is possible for an MPLS VPN customer to monitor a VPN WAN connection using their own CPE functionality at either end with their own internal private network addressing scheme. Their MSP could monitor the same CPEs from their MSP network monitoring system via MPLS PE routers communication with the CPEs on their MPLS network addresses (Nadeau, 2003). The physical access network connection may be provided by either carrier or Tier2 wholesaler. These organisations may have monitoring enabled toward the C-NTE and the A-NTE (see Figure 7).

Various management systems are utilised to administer highly complex communication networks (ITU-T M.3010, 2000; T823, 2004). Many are linked together using SNMP and Extensible Markup Language (XML). For example, element management systems (EMS) manage active network elements. EMS are primarily used for the configuration and management of network elements produced by the same manufacturer (Provencher, 2009). They are relevant in that they often contain SNMP functionality by which the status of network elements they manage may be communicated to a 'northbound' system such as a network management system (NMS) or an Operations Support System (OSS) (Sathyan, 2010). They are primarily utilised by carriers and Tier2 wholesaler organisations. Complex communication networks need to be administered to ensure efficient network management and fault assurance. Standardisation has recommended all major CPs utilise network management systems to oversee the interaction between various networks under their control. These systems often utilise EMS generated data and directly supplied data with which to inform Network Operations Centres

Figure 7. Depiction of varied CP network layers with regard to monitoring



Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

(NOC) of actual and potential issues. NMS often integrate with OSS on 'northbound' interfaces (Wadal and Gupta, 2013).

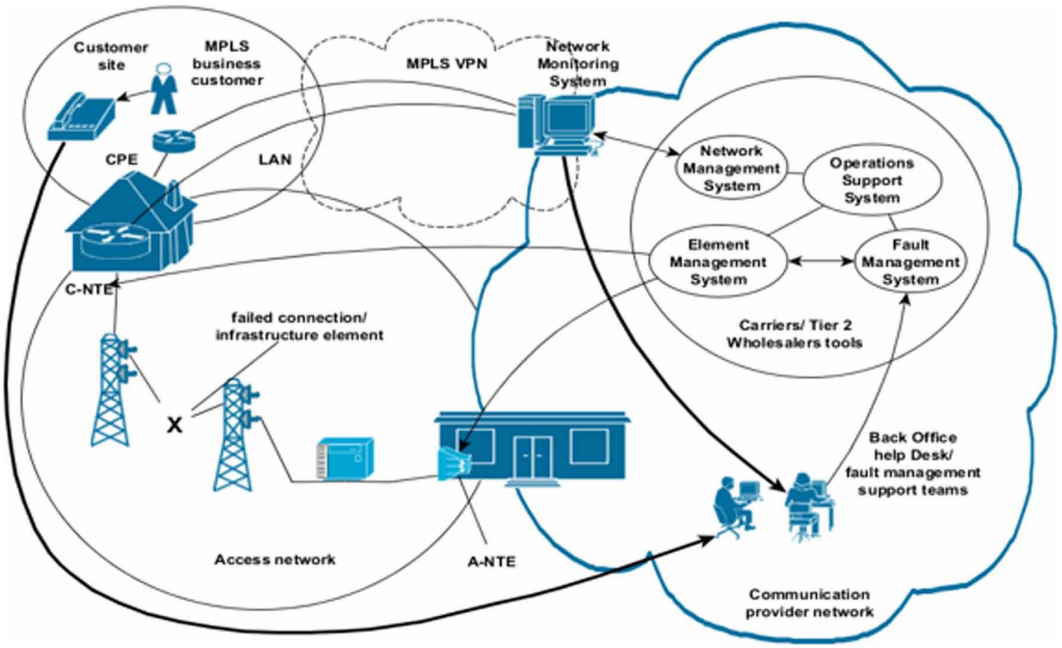
OSS help to collate and disseminate much of the network data of a major CP. Often paired with Business Support Systems (BSS) which deal with the customer side of the business both enable the effective application of FCAPS management functionality (Blum et al, 2008; Orobec, 2010; Saythan, 2010). Openreach's Equivalence Management Platform (EMP) is an example of an integrated OSS/BSS. EMP permits CPs to interact with the Openreach management functions in a variety of manners (Openreach, 2013a). A fact sheet from Openreach illustrates the connection between EMP, a client CPs own systems and active network equipment in the access network (Openreach, 2013b). It is not unusual for larger CPs to operate specific fault management systems (FMS). These may have various roles, such as proactively identifying potential fault locations using data received from DSLAMs and diagnostic tools, Bayesian based systems (Garcia-Algarra et al., 2009) and fault systems used to administer EMS controlled diagnostic tool test-heads.

FMS are utilised by both carrier and Tier2 wholesaler CPs as central points from which to enable remote fault management diagnostics. Often larger CPs own fault management staff and their client CP fault management staff are provided browser-based portal access to FMS. These portal interfaces may have restricted access via Business-to-Business (B2B) integrated Web Gateways or standard website portals such as the BT Wholesale Knowledge Based Diagnostics (KBD) (BTWholesale, 2011). Extensible Markup Language (XML) is the glue that connects many management systems together and enables system interoperability between different CPs (see Figure 8).

2.7. Business-to-Business Interfacing and XML

For accounting and provisioning purposes, carriers and Tier2 Wholesalers connect their management systems together via B2B XML interfacing, presenting seamless automated communication between both organisations (Duke et al., 2006), for example the Openreach B2B Gateway (Openreach, 2013a).

Figure 8. Conceptual depiction of the relationship between management systems and common equipment and functions within the access network



Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

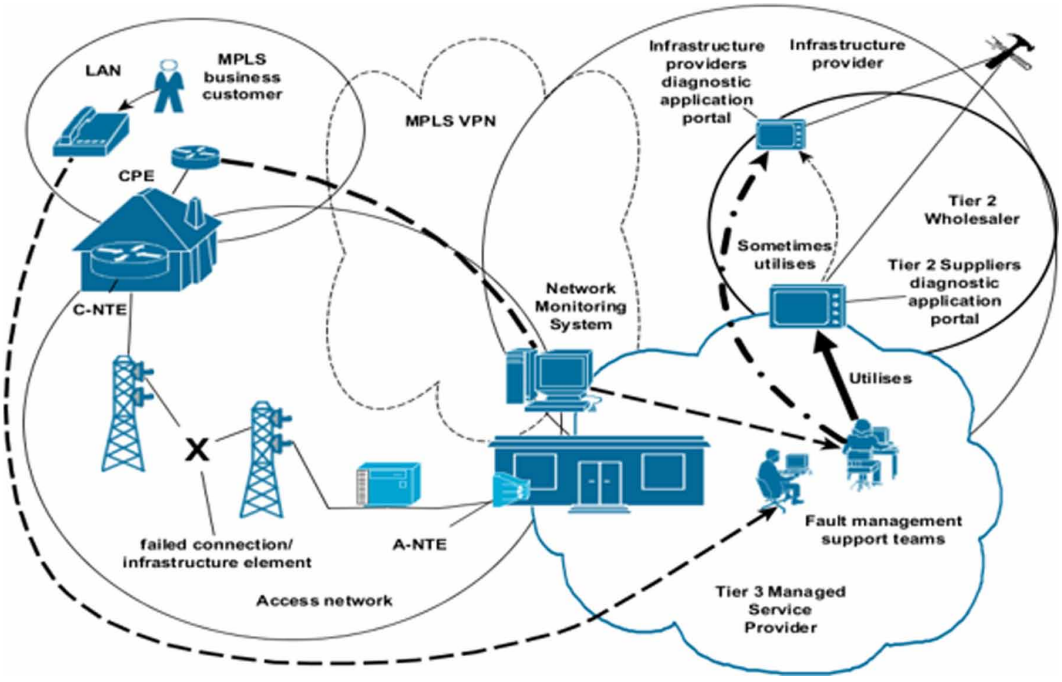
XML enables the configuration of standard scripts that allow systems to interoperate. XML is an example of a non-proprietary Internet Standard technology (see Figure 9).

Diagnostic systems can be utilised via EMS or direct remote access to run diagnostic tests on access network connections. Tests can be run from remote back-office locations or locally to the A-NTE. The results of diagnostic tests are returned as error codes with a description. This study deals only with conclusive diagnostic results such as network disconnections. A diagnostic result will normally indicate the state of a connection from a variety of technical operations and sub-tests. It is possible for tests to detect no power at the CPE for example. In this instance a fail result would not occur since the user may have powered down the equipment onsite to save electricity or for additional security. An actual cut or damage to a cable can be detected though, so a conclusive fail result would be returned.

3. EVALUATION

A key objective was to attain the views of directly affected stakeholders identified as: MPLS VPN solution customers, MPLS MSP Management, and MPLS MSP Fault Management staff. Various research methods and techniques (Sage, 2014) were considered, with the final selection being the use of online-questionnaires as the most appropriate method with which to obtain participant views. Online questionnaires were selected as the most appropriate method to obtain the primary data. Questionnaires are an effective and traditional method used to obtain the views of limited sample populations in specific subjects. Advantages of online questionnaires include low resourcing costs, ease of access for Internet users, and closed questions with limited answer options (Gillham, 2007). Limitations are possible low response, lack of interest from potential participants, and inability to change the design once implemented (Gillham, 2007). The intention was to contact each MSP and

Figure 9. Conceptual illustration of the links between Tier3 MSP fault management team, customer and diagnostic interfaces provided by carrier and Tier2 Wholesalers



Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

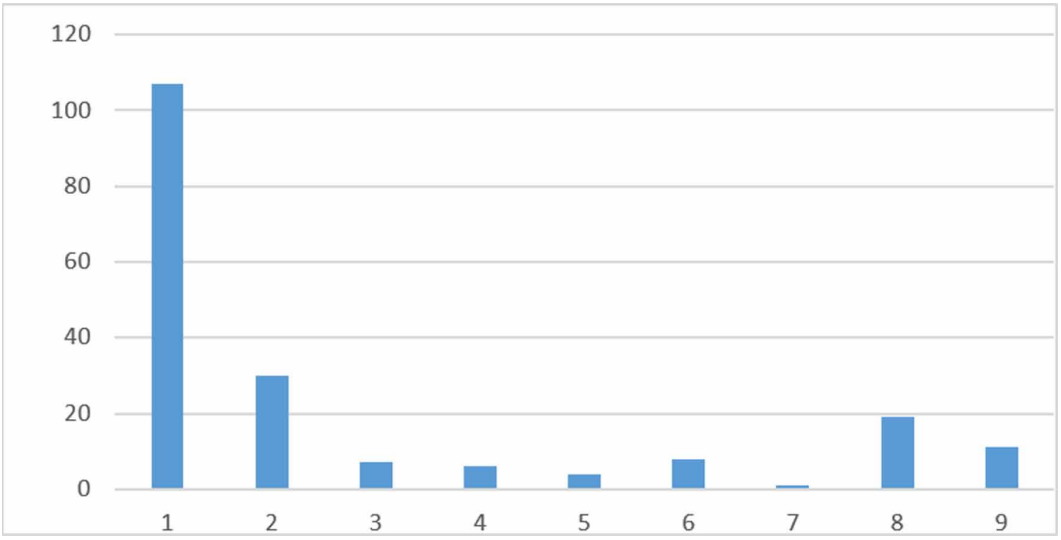
customer organisation by e-mail (Jansen et al., 2007) and telephone to petition their staff to undertake the questionnaires. To mitigate the possibility of low response from the MSP suppliers and customers, two additional online questionnaires were created. These would target additional stakeholder groups: UK public Internet users and UK ISP fault management staff. Links to these questionnaires were posted in UK Web forums. Postal questionnaires were not considered due to high financial costs against a potentially very low response. Interviews in-person, by telephone or by video conferencing were considered but this method would have been overly labour intensive.

102 forum respondents were interested in the questionnaire; 85 were applicable having experienced an outage in the past. 82 respondents completed the first question regarding type of Internet connection technology. The predominant technology was ADSL. 65 respondents answered the remaining questions. When asked how they felt about having to contact their ISP to report the outage, 32 did not have a problem with it, 30 respondents felt annoyed, angry or that time had been wasted and 3 stated that the ISP should not have to be contacted. Asked how they felt about delays when ISP fault management teams initially run manual diagnostics tests 36 respondents did not have issues with the delay, 23 respondents were annoyed, angry or felt time had been wasted and 6 stated that the ISP should not have to be contacted. Respondents were asked how they felt about additional delays in restoring their Internet connection. 18 respondents had no issue with further delays, 38 felt annoyed, angry or that time had been wasted and 1 stated that the ISP should not have to be contacted. 8 had not experienced additional delays. Respondents were asked how they would feel if it were possible to automate the detection, notification and fault management process involved in Internet outages. 20 stated that their feelings would not really change, 29 would feel positive and 16 said they would be impressed. Obtaining willing respondents was a major issue. Due to e-mail spam and unsolicited marketing telephone calls, CPs and business IT staff may easily discard academic survey petition requests such as used here.

The following MSP types were identified by their characteristics and within a total sample of 108 organisations it was found: 107 Tier3 MSPs, 1 International Tier3 MSP, 30 Tier2 Wholesalers, 7 International carriers, 6 National carriers, 4 Regional carriers, 8 Local/specialised carriers, 19 Vertically integrated MSPs and 11 Tier2 Wholesalers and Tier3 MSPs combinations (see Figure 10).

The access connectivity products that these 108 MSP organisations offered are: 67 offered Ethernet (direct), 67 offered EFM, 14 offered FTTP, 56 offered FTTC, 90 offered ADSL, 23 offered

Figure 10. Various MSP types within the Web survey



Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

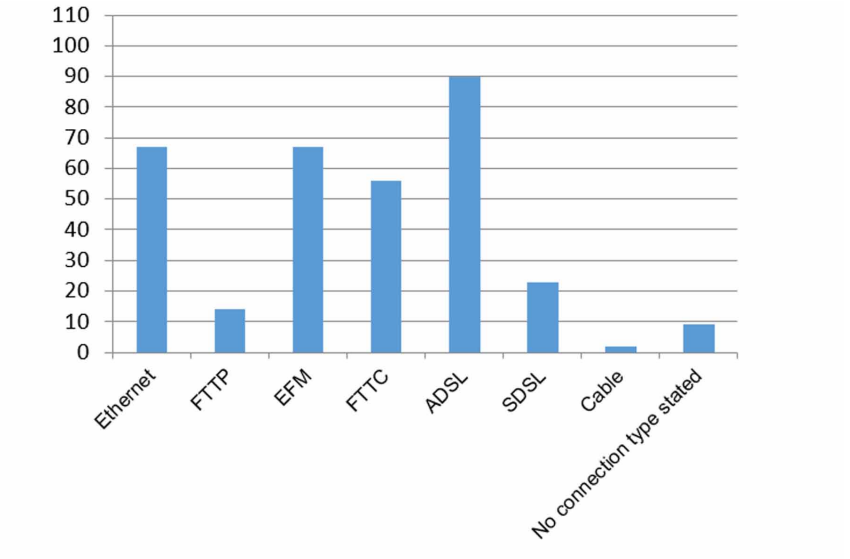
SDSL, 2 offered Cable and 9 did not state which products they offered. Figure 11 depicts the results in diagrammatic format.

Standards can be proprietary or 'Open'. A proprietary standard is developed by a single organisation or small group of organisations which restrict access to the standard from competing organisations. The primary benefit of proprietary standardisation is in maximising market share in a monopolistic manner (Aggarwal et al, 2012). Shah and Kesan (2008) state that users of a proprietary standard are 'locked-in' to a limited number of suppliers with whom they can access the proprietary standard's functionality. In their 2006 article, Aggarwal et al compare proprietary standards to 'pie sharing,' where the monopolistic organisation will attempt to corner as much of the market interested in using products implementing the proprietary standard as possible, whereas Open standards enable 'pie expansion' the ability to earn possibly greater returns by encouraging the number of potential users of the standard to increase. Both Shah and Kesan (2008) and Aggarwal et al (2006) agree Open standards promote interoperability and can potentially reduce costs via increased adoption across the marketplace through competition. Aggarwal et al (2006, 2012) heavily emphasise that Open standards encourage increased adoption of standards by reducing costs for users by increasing the number of potential users. Shah and Kesan (2008) imply that "since the standard is open anyone could implement it". The most relevant aspects of Open standards to this study, that are generally agreed by many interested parties to be basic tenets of Open standards, contributed to the justification to search for non-proprietary Internet Standard technologies:

1. The cost of using the standard should be as low as possible to aid adoption across a potentially greater user base.
2. No specific commercial organisation controls the standard.
3. Change to the standard can be attained through transparent and stakeholder inclusive process.

Many elements and functions of the current system are almost automated. Although SNMP and network monitoring are used to detect last-mile connectivity outages, the protocols involved are inefficient, generating much network traffic. Most carrier and Tier 2 wholesaler fault management is

Figure 11. Access network connectivity products offered by UK MSPs



Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

currently automated and provided to client and own fault management staff via Web system portals. Three areas appear to require some additional functionality to enable full automation.

1. The manual process of fault management staff retrieving circuit details, selecting a diagnostic test and requesting the test via a suppliers Web portal.
2. The lack of inter-organisational fault management system-to-system interfacing.
3. The lack of an effective, lightweight, media independent detection technology.

A Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis follows with regard to high level options for an overall automated solution (Tables 1-4).

Table 1. Option 1 – Design a whole new system from scratch

Strengths	Weaknesses
Could produce a highly efficient solution.	Extremely high costs – developmental, new equipment.
Opportunities	**Threats**
Radical new academic and business opportunities.	Costs outweigh the benefits.

Table 2. Option 2 – Design new components to include with or to replace existing elements of the current system

Strengths	Weaknesses
Simpler and cheaper to implement than a whole new system.	Open to proprietary designs reducing potential distribution
Opportunities	**Threats**
Ability to improve situation in less time and effort than a new system.	Attitude – the cost may outweigh the potential benefits.

Table 3. Option 3 – Use existing internet standard technologies, if available, to improve the situation

Strengths	Weaknesses
Technologies are already standardised, in use, and proven effective. Very cost effective and cheap, no new elements required, possible extensions to existing technologies.	Current elements may not be as efficient and fit effectively as a new elements may be. Elements/technologies may not exist to attain a solution.
Opportunities	**Threats**
Vastly reduced time to research and implement using existing technologies and very low cost to introduce.	Attitude – who cares? Other CP issues are more pressing and require resolving.

Table 4. Option 4 – Continue with no change at all

Strengths	Weaknesses
No costs in time and expense incurred.	Stakeholders will continue to incur losses if no action is undertaken.
Opportunities	**Threats**
The ‘apple cart’ is not upset – no aggrieved/threatened parties.	The perception that the service provider industry may not care about the ‘minimal value’ last-mile customer.

Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

Option 3 was selected where a possible solution may be attainable at low cost with the least change involved and the most potential benefits to the stakeholders. The data gained from the e Public Internet users' questionnaire was analysed and the following noted:

1. An almost equal number of respondents were unaffected by contacting their ISP than were those adversely affected in doing so.
2. Surprisingly, 61% of respondents were not affected by initial ISP diagnostic tests. This appears to indicate an implicit acknowledgment that this manual process is expected.
3. In contrast, about 68% of respondents were negatively affected by additional fault management delays.
4. Some 69% of respondents had positive views toward automation.
5. Of the three questions regarding delays, only 10 responses in 195 indicated that the ISP should not need to be contacted to initiate tests. Possibly results may have been different had there been multiple-choice answers.
6. The information arising from the access connection technology question was expected.

It is difficult however to obtain willing respondents when the validation method requested is via e-mail. There is a natural antipathy to providing e-mails even when data protection has been assured. With the UK Public Internet users' questionnaire validation e-mail addresses were not requested for this reason. Had there been much greater participation from the other questionnaires the information gained from the Public Internet users' questionnaire may have enabled generalisation across all the questionnaires. Many parts of the current system appear to have been automated, specifically in regard to CP fault assurance functions at the carrier and Tier2 wholesaler levels.

1. Carrier and Tier2 Wholesalers already implement B2B system interfacing utilising XML.
2. Enabling FMSs to collate circuit details and select a diagnostic tests would not be difficult to implement.
3. Bi-directional Forwarding Detection is a potential technology that could possibly be utilised to detect last-mile outages.

4. PROPOSED AUTOMATED SOLUTION

Bi-directional Forwarding (BFD) is a simple Hello protocol that is extremely lightweight, very low in bandwidth costs and efficient. It is implemented in backhaul, core and MPLS networks (IETF RFC5884, 2010; Tacca et al., 2006) for rapid detection of outages between forwarding engines and is a non-proprietary draft IETF standard (IETF RFC5880). BFD is able to operate between forwarding engines at any network layer with an underlying connection established (Nordell et al., 2011). BFD is media and technology independent and can operate over any network topology between two BFD enabled forwarding engines. BFD functionality must be installed in a forwarding engine. This could include future versions of CPE, C-NTE and some A-NTE.

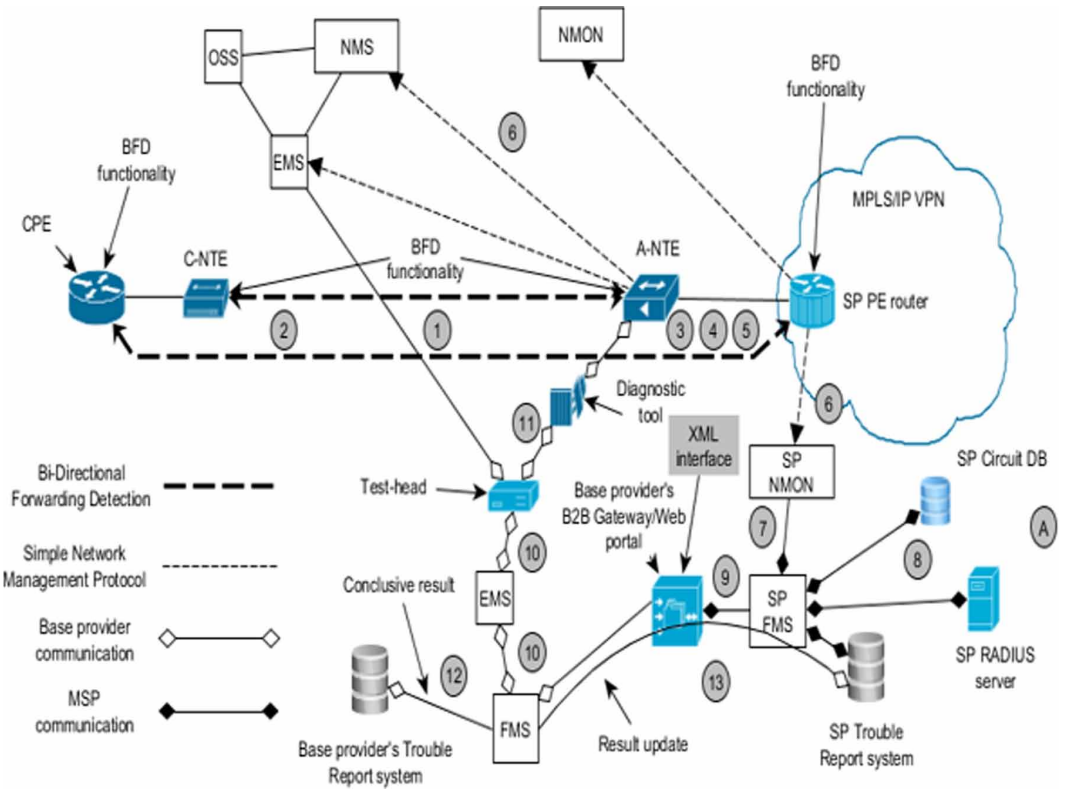
BFD would be used to detect any outage. The current state of BFD can be monitored or managed using existing functionality on the active BFD forwarding engine. With a change in the BFD State, current monitoring or management systems could notify FMS of an outage. To enable automation extending B2B XML interfacing to CP FMSs is recommended. MSPs may need to configure FMSs that would process retrieval of circuit details and request a diagnostic test. Carrier and Tier2 Wholesalers have already automated most of their diagnostic systems allowing client CPs and own staff to use a reduced number of Web portals to manually request tests. With XML technology it should be fairly simple to enable these portals to be incorporated into B2B interfaces. A possible overall solution enabling automation of the process of detection and response is shown in Figure 12.

Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

Figure 12 is an example of a possible automated solution utilising BFD, system-to-system XML fault management interfacing and coded FMSs to process circuit details and results. Referring carrier or Tier2 Wholesaler as the 'Base' provider in the description.

1. Underlying connectivity established between two forwarding engines using a standard connectivity protocol (BFD can work over any encapsulating connection protocol).
2. BFD Hello established between the 'active' forwarding engine (A-NTE/PE) and 'passive' forwarding engine (C-NTE/CPE). The BFD 'State' variable is set to up.
3. Some part of the connection goes down (not via administrative decision), the BFD circuit is dropped. In the case of a single-no backup circuit the passive end is unable to alert the active end that it has stopped receiving BFD packets. The active end is alerted by its own BFD 'Detection timer' value expiring.
4. BFD detection timer expiring causes the BFD state machine to adjust the 'State' variable to down.
5. The BFD active device may wait to see if the connection comes online possibly after a transient issue.
6. The changed value of the BFD 'State' variable acknowledged by management application agents present on the A-NTE/PE. Management agent may wait a set period to allow for restart of remote systems. If BFD state remains down the management agent may alert one of a 'northbound' management system (EMS, NMS, OSS, and NMON).
7. Management/monitoring system informs the MSP FMS of the outage and passes on the network address of the active device interface that was being managed/monitored. This network address

Figure 12. Conceptual design of the proposed solution



Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

will be specific to the MSP involved. If the management/monitoring device knows the network address of the passive device this too may be passed on.
8. The MSP FMS may then retrieve the circuit details for the physical line experiencing the fault from an MSP circuit database.
9. The MSP FMS selects relevant test based on circuit details and request diagnostic testing initiation via Base provider's B2B interface (XML).
10. It is likely that the Base provider has a diagnostic FMS of their own, which connects via EMS to control a large number of diagnostic test-heads. These test-heads can access diagnostic tools attached to A-NTE.
11. The diagnostic tool returns a test result code. The code is sent to the Base provider FMS via test-head and EMS.
12. If the fault is determined to be conclusive then Base provider FMS could automatically create a Base provider trouble report (TR) for truck roll engineer investigation.
13. The Base provider FMS could inform the MSP FMS of the diagnostic test result via B2B interface. MSP FMS may update the MSP Trouble Report system with the result and if the result is inconclusive the MSP's own fault management team can proceed to resolve the fault manually.

The following questions were raised during the Research Definition stage. In answering them an attempt has been made to explain how an automated solution may be attained. How could an automated solution resolve the issue of a number of layered networks with separate network addressing schemes? BFD is able to operate between forwarding engines at any network layer with an underlying connection established (Nordell et al., 2011).

How would an automated solution be able to resolve the disparate nature of?

- The different UK access network technologies currently utilised?

  BFD is media and technology independent.

- The different UK access network topologies involved?

  BFD can operate over any network topology between two BFD enabled forwarding engines.

- The different access network elements involved?

BFD functionality must be installed in a forwarding engine. This could include future versions of CPE, C-NTE and some A-NTE.

How would an automated solution incorporate the diverse detection, monitoring and management functions and tools utilised?

BFD would be used to detect any outage. The current state of BFD can be monitored or managed using existing functionality on the active BFD forwarding engine. With a change in the BFD State, current monitoring or management systems could notify FMS of an outage.

How would an automated system incorporate the various back-office fault management functions and tools utilised?

To enable automation extending B2B XML interfacing to CP FMSs is recommended. MSPs may need to configure FMSs that would process retrieval of circuit details and request a diagnostic test.

How would an automated system incorporate a range of local and remote diagnostic systems?

Carrier and Tier 2 wholesalers have already automated most of their diagnostic systems allowing client CPs and own staff to use a reduced number of web portals to manually request tests. With XML technology it should be fairly simple to enable these portals to be incorporated into B2B interfaces.

Kevin Curran (kj.curran@ulster.ac.uk) Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

An automated solution can be proposed in the event that it is possible for BFD to be utilised in its current implementation or be extended in the manner indicated in figure 12. It should be concluded that this may not be the only possible means by which an automated solution could be attained. This research has indicated that BFD appears to be a viable option in an automated solution, and which matches many of the aspirations behind the research.

The degree to which our aspirations have been attained is dependent on BFD being a suitable technology. If it is:

- Beneficial to a large population – Apart from the introduction of BFD functionality into CPE, C-NTE and A-NTE devices high implementation costs aren't envisaged.
- Can be globally implemented – Being international Internet draft or full standards, BFD and XML are already globally utilised in other related contexts.
- Cheap – BFD and XML are not aggressively proprietary standards. This encourages low cost implementation over a potentially much higher CP user base.
- Effective – BFD and XML are already proven as effective, well received and useful technologies within the CP domain.
- May be extensible to include other fault management functions – Extensibility is an advantage of non-proprietary Internet technologies over proprietary. Most Internet standards have been extended when further useful functionality has been agreed by assorted stakeholders.
- Media and technology independent – The foremost characteristics of both BFD and XML are interoperability with a variety of heterogeneous systems and situations. Both technologies are unconstrained by being tied to specific products.
- Non-proprietary but not necessarily free to use – Both BFD and XML are non-proprietary in the sense that RAND rights enable some income to the original developers.
- Simple to implement – BFD is extremely lightweight requiring very little administration. XML is well established and almost ubiquitous for business system interfacing indicating an ease of use from the uptake of various industries.

Judging this using a minimised CATWOE analysis technique:

- The directly affected stakeholders (Customers) did not express their views collectively.
- Third-party organisations (Actors) were not consulted for their opinions.
- A detailed report as to how such a change could be undertaken (Transformation) was not possible due to word count constraint.
- The ultimate impact (World view) from an automated solution can only be guessed at without a valid survey.
- CPs are the stakeholders (Owners) who would need most convincing about the potential of a solution. These have not provided their views.

5. CONCLUSION

The aim of this research was to assess whether it may be possible to automate the detection and fault management response of common last-mile loss-of-connectivity outages within the access network. It can be concluded that at least one possible automated solution may be attainable in the event that BFD turns out to be a suitable technology. A potential automated solution has been suggested with a summary of how the proposed technologies may mitigate the complexities found within the CP and access network environments under discussion. Rather than CPs being complacent about the end-to-end connection availability of services supplied to their customers, they could be proactive in their stance by implementing an automated detection and fault management solution, potentially

Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

utilising BFD. BFD is already embedded in backhaul and core networks for rapid detection (under 50ms) of outages between two forwarding engines. Perhaps the potential for another novel use for BFD in the access network has not been realised until this time, since the response times for access network outages are much lower than for backhaul and core networks. BFD is beneficial where other the detection functionalities of routing protocols are not, in that it can be routed over a wide variety of networks and technologies whereas routing protocols are often designed with specific network topologies and services in mind.

Similar academic research or current technical documentation was not located where BFD is used in the access network as a connectivity detection tool. Requiring only an established connection between two forwarding engines over which to operate, may enable BFD to be utilised in a wide variety of situations. Combined with automation of B2B fault management interfaces and automated FMS, BFD could be used within large organisational LAN networks, all WAN and Internet connections, legacy and next generation networks, possibly non-terrestrial networks and for fault management within the Internet of Things. BFD could be used to detect intermittent connections and may be extendible to detecting connection performance issues such as jitter and quality of service utilising management agents to record BFD packet round trip time and packet loss. There could be huge potential for all Internet users if the proposed automated solution could be implemented by CPs worldwide. It is very likely that Internet users would look favourably on having their Internet connection detected and diagnosed automatically with no input from themselves to contact their CP. In addition, were they to contact their CP, the CP fault management staff may be able to inform them of the fault diagnostic result and the actions being taken to resolve the outage. For business Internet users the chance of reduced costs incurred due to an outage surely would be very welcome.

Kevin Curran (kj.curran@ulster.ac.uk) Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

REFERENCES

Aggarwal, N., Dai, Q., & Walden, E. (2012). Are open standards good business? *Electronic Markets*, *22*(1), 63–68. doi:10.1007/s12525-011-0078-7

Aggarwal, N., Dai, Q., & Walden, E. A. (2006). Do Markets Prefer Open or Proprietary Standards for XML Standardization? An Event Study. *International Journal of Electronic Commerce*, *11*(1), 117–136. doi:10.2753/JEC1086-4415110105

Almofary, N., Moustafa, H., & Zaki, F. (2013). Scalability Aspects in BGP/MPLS VPN. *International Journal of Modern Engineering Sciences*, *2*, 17–27.

Ayoubi, S., Limam, N., Salahuddin, M. A., Shahriar, N., Boutaba, R., Estrada-Solano, F., & Caicedo, O. M. (2018, January). Machine Learning for Cognitive Network Management. *IEEE Communications Magazine*, *56*(1), 158–165. doi:10.1109/MCOM.2018.1700560

Barker, P. (2009). FTTH Infrastructure: BT Pilot Deployments. In *Proceedings of the 58th IWCS/IICIT International Wire & Cable Symposium* (pp. 133-137). Academic Press.

Beckett, R., Gupta, A., Mahajan, R., & Walker, D. (2017) A General Approach to Network Configuration Verification. In *Proceedings of the Conference of the ACM Special Interest Group on Data Communication ((SIGCOMM)'17)* (pp. 155-168). ACM. doi:10.1145/3098822.3098834

Bendouda, D., & Haffaf, J. (2019). *QFM-MRPL: Towards a QoS and Fault Management based of Mobile-RPL in IoT for mobile applications. In Proceedings of the 15th International Wireless Communications & Mobile Computing Conference* (pp. 354–359). Academic Press. doi:10.1109/IWCMC.2019.8766731

Bharadway, A., Keil, M., & Mahring, M. (2009). Effects of Information Technology Failures on the Market Value of Firms. *The Journal of Strategic Information Systems*, *18*(2).

Biggam, J. (2011). *Succeeding with your Master's Dissertation* (2nd ed.). Maidenhead, UK: Open University Press.

Blum, N., Jacak, P., Schreiner, F., Vingarzan, D., & Weik, P. (2008). Towards Standardized and Automated Fault Management and Service Provisioning for NGNs. *Network and Systems Management*, *16*(1), 63–91. doi:10.1007/s10922-007-9094-5

BT. (2011). *SIN 346 BT ADSL INTERFACE DESCRIPTION.* Retrieved from http://www.sinet.bt.com/sinet/SINs/pdf/346v2p10.pdf

BT. (2013). *SIN 476 BT Downstream 21CN Ethernet Services.* Retrieved from https://www.btwholesale.com/pages/downloads/Products/Integrated_Data_and_Connectivity/SIN_476v1p3.pdf

BTWholesale. (2011). *Introduction to Knowledge Based Diagnostics KBD.* Retrieved from https://www.btwholesale.com/Pages/downloads/Applications/Faults/KBD Handbook v10.0 Release W.pdf

Checkland, P., & Tsouvalis, C. (1997). Reflecting on SSM: The Link between Root Definitions and Conceptual Models. *Systems Research and Behavioral Science*, *14*(3), 153–168. doi:10.1002/(SICI)1099-1743(199705/06)14:3<153::AID-SRES134>3.0.CO;2-H

Cisco. (2007). *Network Management System: Best Practices White Paper.* Retrieved from http://www.cisco.com/c/en/us/support/docs/availability/high-availability/15114-NMS-bestpractice.html

Deljac, Z., Moštak, R., & Stjepanović, T. (2010). The use of Bayesian networks in recognition of faults causes in the BB networks. In *Proceedings of the 33rd International Convention* (pp. 771-775). Academic Press.

Duke, A., Richardson, M., Watkins, S., Wahler, A., & Schreder, B. (2006). Service assurance across organisational boundaries with semantic mediation. *BT Technology Journal*, *24*(1), 153–160. doi:10.1007/s10550-006-0030-0

ETSI. (2003). *ETSI ES 201 488-1 V1.2.2 Access and Terminals (AT) Data Over Cable Systems, European Telecommunications Standards Institute.*

ETSI. (2010). *ETSI TS 101 524 V1.5.1 Access, Terminals, Transmission and Multiplexing (ATTM); Access transmission system on metallic access cables; Symmetric single pair high bitrate; Digital Subscriber Line (SDSL), European Telecommunications Standards Institute*. Retrieved from http://www.etsi.org/deliver/etsi_ts/101500_101599/101524/01.05.01_60/ts_101524v010501p.pdf

Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

ETSI. (2013). *ETSI TS 101 271 V1.2.1 Access, Terminals, Transmission and Multiplexing (ATTM); Access transmission systems on metallic access cables; Very High Speed digital subscriber line system (VDSL2) European Telecommunications Standards Institute*. Retrieved from http://www.etsi.org/deliver/etsi_ts/101200_101299/101271/01.02.01_60/ts_101271v010201p.pdf

Franke, U. (2012). Optimal IT Service Availability: Shorter Outages, or Fewer? *IEEE eTransactions on Network and Service Management*, *9*(1), 22–33. doi:10.1109/TNSM.2011.110811.110122

Garcia-Algarra, F. J., Arozarena-Llopis, P., Garcia-Gomez, S., & Carrera-Barroso, A. (2009). A Lightweight Approach to Distributed Network Diagnosis under Uncertainty. In *Proceedings of the International Conference on Intelligent Networking and Collaborative Systems* (pp. 74-80). doi:10.1109/INCOS.2009.39

Garcia-Gomez, S., & Gonzalez-Ordas, J. Garcia-Algarra, Javier, F., Toribio-Sardon, R., Sedano-Frade, A., (2009). KOWLAN: A Multi Agent System for Bayesian Diagnosis in Telecommunication Networks. In *Proceedings of the IEEE/WIC/ACM International Joint Conferences on Web Intelligence and Intelligent Agent Technologies* (Vol. 3, pp. 195-198). Academic Press.

Ghein, L. D. (2007). *MPLS Fundamentals – A Comprehensive Introduction to MPLS Theory and Practice*. Indianapolis, IN: Cisco Press.

Gill, S., Chana, I., Singh, M., & Buyya, R. (2018). RADAR: Self-configuring and self-healing in resource management for enhancing quality of cloud services. *Concurrency and Computation*, *24*(2), 44–62. doi:10.1002/cpe.4834

Gillham, B. (2007). *Developing a Questionnaire* (2nd ed.). London: Continuum International Publishing Group.

Gunning, P., Wilkinson, M., Rragami, L., Semnani, S., & Smith, K. (2006). Multiservice Ethernet access. *BT Technology Journal*, *24*(2), 72–78. doi:10.1007/s10550-006-0041-x

Hajdarbegovic, N. (2013). German court declares internet is essential - ISP ordered to pay damages for outage. *Techeye*. Retrieved from http://www.techeye.net/internet/german-court-rules-internet-essential-to-life

Holland, O., Ping, S., Aijaz, A., Chareau, J., & Chawdhry, P. (2015). To white space or not to White Space: That is the trial within the Ofcom TV White Spaces pilot. In Proceedings of the 2015 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN). Academic Press. doi:10.1109/DySPAN.2015.7343846

IETF. (2001) *RFC3031 Multiprotocol Label Switching Architecture,* Internet Engineering Task Force. Retrieved from http://tools.ietf.org/html/rfc3031

IETF. (2006) *RFC4364 BGP/MPLS IP Virtual Private Networks (VPNs),* Internet Engineering Task Force. Retrieved from http://www.ietf.org/rfc/rfc4364.txt

IETF. (2006) *RFC4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*, Internet Engineering Task Force. Retrieved from http://tools.ietf.org/html/rfc4379

IETF. (2008) *RFC5286 Basic Specification for IP Fast Reroute: Loop-Free Alternates*, Internet Engineering Task Force. Retrieved from http://tools.ietf.org/html/rfc5286

IETF. (2010) *RFC5880 Bidirectional Forwarding Detection (BFD), Internet Engineering Task Force*. Retrieved from http://tools.ietf.org/html/rfc5880

IETF. (2010) *RFC5884 Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs*). Internet Engineering Task Force. Retrieved from http://tools.ietf.org/html/rfc5884

IETF. (2011) *RFC6291 Guidelines for the Use of the "OAM" Acronym in the IETF*, Internet Engineering Task Force. Retrieved from http://tools.ietf.org/html/rfc6291

ITU-T. (1992) *X.700: Management framework for Open Systems Interconnection (OSI) for CCITT applications*, International Telecommunications Union. Retrieved from https://www.itu.int/rec/T-REC-X.700-199209-I/en

ITU-T. (1999) *G.992.1: Asymmetric digital subscriber line (ADSL) transceivers,* International Telecommunications Union. Retrieved from https://www.itu.int/rec/T-REC-G.992.1-199907-I/en

ITU-T. (2000) *M.3010: Principles for a telecommunications management network*, International Telecommunications Union. Retrieved from http://www.itu.int/rec/T-REC-M.3010

Kevin Curran (kj.curran@ulster.ac.uk) Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

ITU-T. (2000) *M.3400: TMN management functions*, International Telecommunications Union. Retrieved from https://www.itu.int/rec/T-REC-M.3400-200002-I/en

ITU-T. (2005) *G.991.2: Single-pair high-speed digital subscriber line (SHDSL) transceivers*, International Telecommunications Union. Retrieved from https://www.itu.int/rec/T-REC-G.991.2/en

ITU-T. (2008) *G.984.1: Gigabit-capable passive optical networks (GPON): General characteristics,* International Telecommunications Union. Retrieved from https://www.itu.int/rec/T-REC-G.984.1/en

ITU-T. (2009) *G.992.: Asymmetric digital subscriber line 2 transceivers (ADSL2) - Extended bandwidth ADSL2 (ADSL2plus)*, International Telecommunications Union. Retrieved from https://www.itu.int/rec/T-REC-G.992.5/en

ITU-T. (2013) *Y.1731: OAM functions and mechanisms for Ethernet based networks*, International Telecommunications Union. Retrieved from https://www.itu.int/rec/T-REC-Y.1731/en

Jansen, K., Corley, K., & Jansen, B. (2007). *"E-Survey Methodology", Handbook of Research on Electronic Surveys and Measurements*. Chicago: Idea Group Inc.

Jin, Y., Gerber, A., Haffner, P., Sen, S., & Zhang, Z. (2010). NEVERMIND, the Problem is Already Fixed: Proactively Detecting and Troubleshooting Customer DSL Problems. In *Proceedings of the 6th International Conference Co-NEXT '10*. New York: ACM. doi:10.1145/1921168.1921178

Jones, R. (2004). *T823 Block 6: Network Management*. Milton Keynes: Open University.

Jones, R., Bisell, C., & Reed, D. (2003). *T822 Block 2: Communication Architectures*. Milton Keynes: Open University.

Kerpez, K. J., & Kinney, R. (2008). Integrated DSL test, analysis, and operations. *IEEE Transactions on Instrumentation and Measurement*, *57*(4), 770–780.

Kim, K.-H., Singh, V., & Schulzrinne, H. G. (2011). *DYSWIS: Collaborative Network Fault Diagnosis - Of End-users, By End-users, For End-users*. Retrieved from http://hdl.handle.net/10022/AC:P:10672

Knowles, R. (2013). Businesses without phone and internet connection for two weeks. *Guardian*. Retrieved from http://www.guardianseries.co.uk/news/10796870.Businesses_without_phone_and_internet_connection

Kompella, R., Yates, J., Greenberg, A., & Snoeren, A. (2010). Fault localization via risk modeling. *IEEE Transactions on* Dependable and Secure Computing, *7*(4), 396–409.

Lee, S., & Kim, H. S. (2012). End-user perspectives of Internet connectivity problems. *Computer Networks*, *56*(6), 1710–1722. doi:10.1016/j.comnet.2012.01.009

Lewis, C., & Pickavance, S. (2006). *Selecting MPLS VPN Services*. Indianapolis: Cisco Press.

Li, S., & Liang, H. (2011). A model of path fault recovery of MPLS VPN and simulation. In *Proceedings of the 2011 International Conference on Electric Information and Control Engineering (ICEICE)* (pp. 1925–1928). Academic Press. doi:10.1109/ICEICE.2011.5777806

Li, Y., Cui, W., Li, D., & Zhang, R. (2011). Research based on OSI model. In *Proceedings of the IEEE 3rd International Conference on Communication Software and Networks (ICCSN)* (pp. 554-557). IEEE Press. doi:10.1109/ICCSN.2011.6014631

Lyons, S., Morgenroth, E., & Tolc, R. S. J. (2012). Estimating the value of lost telecoms connectivity. *Electronic Commerce Research and Applications*, *12*(1), 40–51. doi:10.1016/j.elerap.2012.06.002

McGuire, A. (2008). *Next Generation Ethernet. In The Cable and Telecommunications Professionals' Reference Transport Networks*. Burlington: Elsevier Inc.

MEF-17. (2007). *Technical Specification, MEF 17, Service OAM Requirements & Framework – Phase 1*. Retrieved from https://www.metroethernetforum.org/Assets/Technical_Specifications/PDF/MEF17.pdf

Minei, I., & Lucek, J. (2011). *MPLS-Enabled Applications*. Chichester: Wiley.

Nadeau, T. (2003). *MPLS Network Management*. San Francisco: Elsevier Science.

Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

Nordell, V., Gavler, A., & Skoldstrom, P. (2011). BFD triggered, GMPLS based multi-layer Ethernet access network protection. In *Proceedings of the Communications and Photonics Conference and Exhibition*. Academic Press.

Nyasulu, T., Crawford, D., & Mikeka, C. (2018). Malawi's TV white space regulations: A review and comparison with FCC and Ofcom regulations. In *Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE Press. doi:10.1109/WCNC.2018.8377175

Ofcom. (2012). *Boosting business telecoms to meet growing demand for data*. Retrieved from http://m.ofcom.org.uk/media/news-releases/growing-data-demand/

Ofcom. (2013a). *Fixed access market reviews: wholesale local access, wholesale fixed analogue exchange lines, ISDN2 and ISDN30*. Retrieved from http://stakeholders.ofcom.org.uk/consultations/fixed-access-market-reviews/

Openreach. (2011a). *Fact sheet: Local Loop Unbundling (LLU) for Metallic Path Facility (MPF)*. Retrieved from http://www.openreach.co.uk/orpg/home/products/llu/mpf/mpf/downloads/71743_llu_mpf_factsheet_update_03_phme71743_web.pdf

Openreach. (2013a). *Equivalence Management Platform (EMP)-a high level overview*. Retrieved from http://www.openreach.co.uk/orpg/home/products/downloads/EMPHighLevelViewv23.pdf

Openreach. (2013b). *Fact sheet: Fibre Voice Access over Fibre to the Premises*. Retrieved from http://www.openreach.co.uk/orpg/home/products/super-fastfibreaccess/fibrevoiceaccess/fibrevoiceaccess/downloads/FVA_263348 20111108.pdf

Openreach. (2014). *Duct and Pole sharing*. Retrieved from http://www.openreach.co.uk/orpg/home/products/ductandpolesharing/ductandpolesharing.do

Orobec, S. (2010). *Next Generation OSS Architecture. In Next generation telecommunications networks, services, and management*. Hoboken, NJ: IEEE Press Series on Network Management.

Provencher, D. (2009). Operations Automation Using NETSMART 1500 Element Manager. *Fujitsu Scientific and Technical Journal*, *45*(4), 422–430.

Reed, D. (2003). *T822 Block 1: Protocols*. Milton Keynes: Open University.

Rios, E., Iturbe, E., & Palacios, M. (2017). Self healing multicloud application modelling. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*. Academic Press. doi:10.1145/3098954.3104059

Sabatucci, L., Lopes, S., & Cossentino, M. (2017). Self-configuring cloud application mashup with goals and capabilities. *Cluster Computing*, *20*(3), 2047–2063. doi:10.1007/s10586-017-0911-7

Sage. (n.d.). *SAGE Research Methods.* Retrieved from srmo.sagepub.com.libezproxy.open.ac.uk

Sathyan, J. (2010). *Fundamentals of EMS, NMS and OSS/BSS*. Boca Raton: Auerbach Publication.

Shah, R., & Kesan, J. P. (2008). An Empirical Examination of Open Standards Development. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences* (p. 212). Academic Press. doi:10.1109/HICSS.2008.49

Singh, S., Chana, I., & Buyya, R. (2017). STAR: SLA aware autonomic management of cloud resources. *IEEE Trans Cloud Comput.*, *4*, 1–14. doi:10.1109/TCC.2017.2648788

Stenbjerg, J., Beck Krogh, T., Madsen, J., & Schmid, S. (2018). P-Rex: fast verification of MPLS networks with multiple link failures. In *Proceedings of the 14th International Conference on emerging Networking Experiments and Technologies CoNEXT '18* (pp. 217–227). Academic Press. doi:10.1145/3281411.3281432

Sullivan, M. A., Klein, A. L., McAfee, W., Scott, C., & Wilburn, D. E., Jr. (2009). U.S. Patent No. 7,518,991. Washington, DC: U.S. Patent and Trademark Office.

Sundaresan, S., Donato, W., Feamster, N., Teixeira, R., Crawford, S., & Pescapè, A. (2011). Broadband Internet Performance: A View from the Gateway. In *Proceedings of the ACM SIGCOMM 2011 Conference SIGCOMM '11* (pp. 134–145). New York: ACM. doi:10.1145/2018436.2018452

Kevin Curran (kj.curran@ulster.ac.uk)
Downloaded: 4/23/2021 9:47:47 AM
IP Address: 92.20.186.168

Tacca, M., Wu, K., Fumagalli, A., & Vasseur, J. P. (2006). Local Detection and Recovery from Multi-Failure Patterns in MPLS-TE Networks. In *Proceedings of the IEEE International Conference on Communications ICC 06* (pp. 658–663). IEEE. doi:10.1109/ICC.2006.254782

Turner, D., Levchenko, K., Mogul, J., Savage, S., & Snoeren, A. (2012). *On Failure in Managed Enterprise Networks*. Retrieved from http://www.hpl.hp.com/techreports/2012/HPL-2012-101.pdf

Wadal, P., & Gupta, S. (2013). An Overview of Network Management System. *International Journal of Computer Science and Applications*, *6*(2), 337–341.

Kevin Curran is a Professor of Cyber Security, Executive Co-Director of the Legal innovation Centre and group leader of the Cyber Security and Web Technologies Research Group at Ulster University. His achievements include winning and managing UK & European Framework projects and Technology Transfer Schemes. Professor Curran has made significant contributions to advancing the knowledge and understanding of computer networks and security, evidenced by over 800 published works. His expertise has been acknowledged by invitations to present his work at international conferences, overseas universities and research laboratories. He is a regular contributor to print, online, radio & TV news on computing & security issues. He was the recipient of an Engineering and Technology Board Visiting Lectureship for Exceptional Engineers and is an IEEE Public Visibility technical expert since 2008. He currently holds a Royal Academy of Engineering/Leverhulme Trust Senior Research Fellowship awarded in 2016. Professor Curran's stature and authority in the international community is demonstrated by his influence, particularly in relation to the direction of research in computer science. He has chaired sessions and participated in the organising committees for many highly-respected international conferences and workshops. He was the founding Editor in Chief of the International Journal of Ambient Computing and Intelligence and is also a member of numerous Journal Editorial boards and international conference organising committees. He has authored a number of books and is the recipient of various patents. He has served as an advisor to the British Computer Society in regard to the computer industry standards and is a member of BCS and IEEE Technology Specialist Groups and various other professional bodies. https://kevincurran.org